David J. Molton (admitted *pro hac vice*)
Gerard T. Cicero
BROWN RUDNICK LLP
Seven Times Square
New York, New York 10036
Telephone: (212) 209-4800
Facsimile: (212) 209-4801
Email: dmolton@brownrudnick.com
Email: gcicero@brownrudnick.com

- and –

Thomas Scannell (TX 24070559)
FOLEY & LARDNER LLP
2021 McKinney Avenue
Dallas, Texas 75201
Telephone: (214) 999-4289
Email: tscannell@foley.com

Counsel for Nobuaki Kobayashi,
In His Capacities as the Bankruptcy Trustee
and Foreign Representative and Trustee of the
Second Civil Rehabilitation Proceeding
and Foreign Representative of MtGox Co., Ltd.,
a/k/a MtGox KK

IN THE UNITED STATES BANKRUPTCY COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

In re:	Chapter 15
MTGOX Co., LTD. (a/k/a MTGOX KK),	Case No. 14-31229-sgj-15
Debtor in a Foreign Proceeding.	

NOBUAKI KOBAYASHI IN HIS CAPACITY AS FOREIGN REPRESENTATIVE STATUS UPDATE

Nobuaki Kobayashi, in his capacities as the bankruptcy trustee and foreign representative (the "Trustee") of MtGox Co., Ltd., a/ka/ MtGox KK (the "Debtor") and as the trustee of the Second Civil Rehabilitation Proceeding and foreign representative of the Debtor in connection with that proceeding, by and through his United States attorneys, Brown Rudnick LLP and Foley

& Lardner LLP, hereby submits a status update concerning the Government's criminal prosecution and civil action against Alexander Vinnik and BTC-e.

STATUS UPDATE

A. The Government's Efforts to Prosecute Alexander Vinnik and BTC-e

1. The Trustee is aware of two pending actions against Alexander Vinnik and BTC-e, both of which were initiated by the U.S. Attorney's Office for the Northern District of California (the "Government"), and which stem from Vinnik and BTC-e's involvement in a series of hacking incidents concerning the Mt. Gox bitcoin exchange between approximately 2011 and 2014.

2. The first action is a criminal prosecution, *United States of America v. BTC-e and Vinnik,* N.D. Cal., Case No CR 16-00227 (SI) (Jan. 17, 2017) (sealed) (the "Criminal Case"). The indictment[1] charges BTC-e and Vinnik with one count of operation of an unlicensed money service business, in violation of 18 U.S.C. § 1960, and one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h). In addition, the indictment charges Vinnik with seventeen counts of money laundering, in violation of 18 U.S.C. § 1956(a)(1), and two counts of engaging in unlawful monetary transactions, in violation of 18 U.S.C. § 1957. The indictment also contains a criminal forfeiture allegation pursuant to 18 U.S.C. § 982(a)(1).

3. The indictment alleges that Vinnik operated and controlled BTC-e, and that after that Mt. Gox hack, approximately "530,000 of the bitcoin . . . stolen from Mt. Gox was deposited into wallets at three different digital currency exchanges [including] BTC-e . . . ." Indictment ¶ 52. The proceedings in this action remain sealed.

[1] The criminal indictment is the only publicly available filing, and is attached hereto as Exhibit A.

4. The second action is a civil action, *United States of America v. BTC-e and Vinnik,* N.D. Cal., Case No 19-CV-04281 (KAW) (Jul. 25, 2019) (the "Civil Case").[2] The complaint in the Civil Case reflects an action to "recover civil money penalties imposed under the Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §§ 5311-5314, and 5316-5332, which is commonly referred to as the Bank Secrecy Act."

5. The Civil Case seeks a judgment against BTC-e and Vinnik for failure to register BTC-e as a "Money Service Business," for failure to "develop, implement, and maintain an effective [Anti-Money Laundering] program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities," and for failure to files Suspicious Activity Reports. *See* Complaint at ¶¶ 31-38. Further, the Civil Case notes that FinCEN imposed on BTC-e and Vinnik "civil monetary penalties in the amounts of $88,596,314 and $12,000,000, respectively" for such violations. *See id.*, ¶ 40; Ex. 1 to Complaint (FinCEN Assessment of Civil Money Penalty).

B. Current Status of Vinnik as Foreign Prisoner

6. As of the date of this filing, Vinnik is currently serving a prison term in France in connection with violations of French law, and there have been recent reports of his potential release and extradition, either to Greece, the United States, or Russia, where Vinnik faces further criminal prosecution.[3]

7. Throughout the last several years, the Government has, upon information and belief, sought to extradite Vinnik to the United States, and effectuate service of the Civil Complaint on Vinnik and BTC-e. In a May 18, 2022 Status Report filed by the Government in the Civil

[2] Attached hereto as Exhibit B is the complaint in the Civil Case.

[3] Lubomir Tassev, *Alexander Vinnik Serves Prison Term in France but No Freedom in Sight*, BITCOIN.COM, Jun. 6, 2022, https://news.bitcoin.com/alexander-vinnik-serves-prison-term-in-france-but-no-freedom-in-sight/

Case,[4] the Government confirmed that service is complete via Federal Rule of Civil Procedure 4(f)(1) and the Hague Service Convention. Vinnik and BTC-e have not appeared in the case, nor have they filed a responsive pleading to the Government's complaint. The Government reports that is "intends to seek entry of default against Defendants . . . no later than July 18, 2022." *See* Status Report at 2.

C. The Trustee's Interest in the Civil Case and Criminal Case

8. The Trustee has diligently monitored the proceedings concerning Vinnik and BTC-e, including direct correspondence with the Government concerning requests for information on the hack of Mt. Gox and Vinnik's involvement, developments of Vinnik's extradition, and specifically, the Government's intention to initiate civil and/or criminal forfeiture proceedings against Vinnik and BTC-e, in the event that the Government obtains a default judgment. The Trustee maintains that it has a property interest in any and all bitcoin stolen or impermissibly transferred by Vinnik or his agents from Mt. Gox and has informed the United States of such property interests and of this Bankruptcy Case. The Trustee intends to take all actions necessary and proper in order to recover the bitcoin recovered from Vinnik, his agents or BTC-e and has informed the United States of this intent to do so in accordance with 11 U.S.C. § 1521(a)(5).

9. Given the current status of the Civil Case and Criminal Case, including Vinnik's extradition, the Trustee reserves all rights to seek relief from this Court to effectuate or otherwise protect the Trustee's interests in any such bitcoin or fiat currency in Vinnik and BTC-e's possession that was stolen from Mt. Gox, and which would, upon information and belief, be subject to any future Government's forfeiture proceedings.

[4] Attached hereto as Exhibit C.

Dated: July 14, 2022
Dallas, Texas

Respectfully submitted,

FOLEY &LARDNER LLP

/s/ Thomas C. Scannell
Thomas Scannell (TX 24070559)
2021 McKinney Avenue
Dallas, Texas 75201
Telephone: (214) 999-4289
Email: tscannell@foley.com

- and –

BROWN RUDNICK LLP
David J. Molton (admitted *pro hac vice*)
Gerard T. Cicero
Seven Times Square
New York, New York 10036
Telephone: (212) 209-4800
Facsimile: (212) 209-4801
Email: dmolton@brownrudnick.com
Email: gcicero@brownrudnick.com

Counsel for Nobuaki Kobayashi,
In His Capacities as the Bankruptcy Trustee and Foreign Representative and Trustee of the Second Civil Rehabilitation Proceeding and Foreign Representative of MtGox Co., Ltd., a/k/a MtGox KK

CERTIFICATE OF SERVICE

The undersigned hereby certifies a true and correct copy of the foregoing was served on July 14, 2022 in compliance with the Federal Rules of Bankruptcy Procedure via the Court's CM/ECF electronic service protocols on all parties registered to receive electronic notice in the above-captioned bankruptcy case.

/s/ Thomas C. Scannell
Thomas C. Scannell

EXHIBIT A

BRIAN J. STRETCH (CABN 163973)
United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

WIL FRENTZEN (LABN 24421)
Assistant United States Attorney
450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6959
Fax: (415) 436-7234
William.Frentzen@usdoj.gov

Attorneys for the United States

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-E, A/K/A CANTON BUSINESS CORPORATION, and ALEXANDER VINNIK. Defendants.	CASE NO: CR 16-00227 SI UNITED STATES' MOTION TO SEAL SUPERSEDING INDICTMENT, ARREST WARRANTS AND ~~[PROPOSED]~~ ORDER UNDER SEAL

The United States hereby moves the Court for an order sealing this Motion and Order, Arrest Warrants and the Superseding Indictment. The government believes that if the defendants are made aware of these documents before they are arrested, that they may make efforts to avoid being arrested.

Date: January 17, 2017

Respectfully Submitted,

BRIAN J. STRETCH
United States Attorney

WILLIAM FRENTZEN
Assistant United States Attorney

[~~PROPOSED~~] ORDER

Based upon the foregoing request, the Court hereby **ORDERS** that this Motion and Order, Arrest Warrants and the Superseding Indictment shall be filed and kept under seal by the clerk of the Court until further order of the Court. The Court hereby further **ORDERS** that any representative of the United States Attorney's Office or the Internal Revenue Service, shall be allowed to obtain a copy of the Superseding Indictment without further order of the Court.

Dated: January 17, 2017

HON. SALLIE KIM
UNITED STATES MAGISTRATE JUDGE

United States District Court

FOR THE
NORTHERN DISTRICT OF CALIFORNIA

VENUE: SAN FRANCISCO

UNITED STATES OF AMERICA,

V.

SEALED
BY COURT ORDER

CR16-0227-SI

BTC-E, A/K/A CANTON BUSINESS CORPORATION
and ALEXANDER VINNIK,

DEFENDANT(S).

SUPERSEDING INDICTMENT

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business;
18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering;
18 U.S.C. § 1956(a)(1) - Money Laundering;
18 U.S.C. § 1957 - Unlawful Monetary Transactions; and
18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

A true bill.

Foreman

Filed in open court this 17th day of

January, 2017

Clerk

SALLIE KIM
United States Magistrate Judge

NO BAIL WARRANT
for Alexander Vinnik

NO PROCESS for BTC-E

Bail, $

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT ☒ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

OFFENSE CHARGED

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) - Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

☐ Petty ☐ Minor ☐ Misdemeanor ☒ Felony

PENALTY: Please see attachment.

SEALED BY COURT ORDER

DEFENDANT - U.S

BTC-E, A/K/A CANTON BUSINESS CORPORATION

DISTRICT COURT NUMBER

CR 16-00227 SI

FILED
JAN 17 2017
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)

Internal Revenue Service

☐ person is awaiting trial in another Federal or State Court, give name of court

_____

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

_____

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of: ☐ U.S. ATTORNEY ☐ DEFENSE } SHOW DOCKET NO. _____

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under } MAGISTRATE CASE NO. _____

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges _____

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

_____

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

_____

Has detainer been filed? ☐ Yes ☐ No } If "Yes" give date filed _____

DATE OF ARREST ▶ Month/Day/Year _____

Or... If Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year _____

Name and Office of Person Furnishing Information on this form BRIAN J. STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) WILLIAM FRENTZEN

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount: _____

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

Defendant Address:

_____

Date/Time: _____ Before Judge: _____

Comments:

ATTACHMENT TO PENALTY SHEET

BTC-E, A/K/A CANTON BUSINESS CORPORATION

COUNT ONE: (18 U.S.C. §1960 – Operation of an Unlicensed Money Service Business)

5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

AO 257 (Rev. 6/78)

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ COMPLAINT ☐ INFORMATION ☒ INDICTMENT ☒ SUPERSEDING

Name of District Court, and/or Judge/Magistrate Location

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

OFFENSE CHARGED

18 U.S.C. § 1960 - Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) - Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) - Money Laundering; 18 U.S.C. § 1957 - Unlawful Monetary Transactions; and 18 U.S.C. §§ 982(a)(1) - Criminal Forfeiture

☐ Petty ☐ Minor ☐ Misde-meanor ☒ Felony

PENALTY: Please see attachment.

SEALED BY COURT ORDER

DEFENDANT - U.S

▶ ALEXANDER VINNIK

DISTRICT COURT NUMBER

CR 16-00227 SI

FILED JAN 17 2017 SUSAN Y. SOONG CLERK, U.S. DISTRICT COURT NORTHERN DISTRICT OF CALIFORNIA

PROCEEDING

Name of Complaintant Agency, or Person (& Title, if any)

Internal Revenue Service

☐ person is awaiting trial in another Federal or State Court, give name of court

☐ this person/proceeding is transferred from another district per (circle one) FRCrp 20, 21, or 40. Show District

☐ this is a reprosecution of charges previously dismissed which were dismissed on motion of: ☐ U.S. ATTORNEY ☐ DEFENSE } SHOW DOCKET NO.

☐ this prosecution relates to a pending case involving this same defendant

☐ prior proceedings or appearance(s) before U.S. Magistrate regarding this defendant were recorded under } MAGISTRATE CASE NO.

Name and Office of Person Furnishing Information on this form BRIAN J. STRETCH

☒ U.S. Attorney ☐ Other U.S. Agency

Name of Assistant U.S. Attorney (if assigned) WILLIAM FRENTZEN

DEFENDANT

IS *NOT* IN CUSTODY

1) ☒ Has not been arrested, pending outcome this proceeding. If not detained give date any prior summons was served on above charges ▶

2) ☐ Is a Fugitive

3) ☐ Is on Bail or Release from (show District)

IS IN CUSTODY

4) ☐ On this charge

5) ☐ On another conviction } ☐ Federal ☐ State

6) ☐ Awaiting trial on other charges

If answer to (6) is "Yes", show name of institution

Has detainer been filed? ☐ Yes ☐ No } If "Yes" give date filed

DATE OF ARREST ▶ Month/Day/Year

Or... If Arresting Agency & Warrant were not

DATE TRANSFERRED TO U.S. CUSTODY ▶ Month/Day/Year

☐ This report amends AO 257 previously submitted

ADDITIONAL INFORMATION OR COMMENTS

PROCESS:

☐ SUMMONS ☐ NO PROCESS* ☒ WARRANT Bail Amount:

If Summons, complete following:

☐ Arraignment ☐ Initial Appearance

Defendant Address:

Date/Time: Before Judge:

Comments:

** Where defendant previously apprehended on complaint, no new summons or warrant needed, since Magistrate has scheduled arraignment*

ATTACHMENT TO PENALTY SHEET

ALEXANDER VINNIK

COUNT ONE: (18 U.S.C. §1960 – Operation of an Unlicensed Money Service Business)

5 years imprisonment

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

Not more than 20 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) - Money Laundering)

Not more than 20 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

Not more than 10 years imprisonment; not more than $500,000 fine or twice the value of the property involved in the transaction, whichever is greater; not more than 3 years of supervised release; and a $100 special assessment.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

BRIAN J. STRETCH (CABN 163973)
United States Attorney

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-E, A/K/A CANTON BUSINESS CORPORATION, and ALEXANDER VINNIK. Defendants.	UNDER SEAL CASE NO. CR 16-00227 SI VIOLATIONS: 18 U.S.C. § 1960 – Operation of an Unlicensed Money Service Business; 18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering; 18 U.S.C. § 1956(a)(1) – Money Laundering; 18 U.S.C. § 1957 – Unlawful Monetary Transactions; 18 U.S.C. § 982(a)(1) – Criminal Forfeiture SAN FRANCISCO VENUE

SUPERSEDING INDICTMENT

The Grand Jury charges:

INTRODUCTORY ALLEGATIONS

At all times relevant to this Indictment:

1. Since at least approximately 2011 through and including the present, both dates being approximate and inclusive, the defendant BTC-e operated as one of the world's largest and most widely used digital currency exchanges. Since its inception, BTC-e processed several billion dollars worth of monetary exchanges. BTC-e was an exchange for cybercriminals worldwide, and one of the principal entities used to launder and liquidate criminal proceeds from digital currencies, including Bitcoin, to fiat

currencies,[1] including U.S. dollars, Euros, and Rubles. At all relevant times, the defendant ALEXANDER VINNIK, together with individuals known and unknown, directed and supervised BTC-e's operations and finances.

2. BTC-e was an international money-laundering scheme that, by virtue of its business model, catered to criminals – and to cybercriminals in particular. Through VINNIK's efforts, BTC-e emerged as one of the principal means by which cyber criminals around the world laundered the proceeds of their illicit activity. BTC-e facilitated crimes, including computer hacking and ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking.

3. BTC-e lacked basic anti-money laundering controls and policies and, as such, was attractive to those who desired to conceal criminal proceeds as it made it more difficult for law enforcement to trace and attribute funds.

4. Since its founding, BTC-e received criminal proceeds of numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. Among other things, BTC-e accounts received substantial proceeds from the hack of the now-defunct Mt. Gox digital currency exchange and also received a substantial portion of the criminal proceeds from one of the largest ransomware schemes, CryptoWall.

5. As described further below, the defendants and their co-conspirators, including those known and unknown to the Grand Jury, intentionally created, structured, and operated BTC-e as a criminal business venture, one designed to help criminals launder their proceeds and one they themselves used to launder criminal proceeds. The defendants thus attracted and maintained a customer base that was heavily reliant on criminals.

6. Despite doing substantial business in the United States, BTC-e was not registered as a

[1] Fiat currency is simply a currency established by government regulation or law, e.g. U.S. Dollars, Euros, Japanese Yen, British Pounds, Russian Rubles, Chinese RMB, etc.

money services business with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), as federal law requires. As described further below, BTC-e had no meaningful anti-money laundering processes in place and lacked an effective anti-money laundering program, as federal law also requires.

7. This was in contrast to other registered digital currency exchanges that, through their anti-money laundering programs, strove to avoid having their platforms used for criminal activity. Most of those exchanges described their operations down to listing the names, photos, and backgrounds of their management, the location of their businesses, and their regulatory compliance policies.

8. BTC-e relied on the use of shell companies and affiliate entities that were similarly unregistered with FinCEN and lacked basic anti-money laundering and "Know Your Customer" policies. These entities catered to an online and worldwide customer base, and electronically "muled" fiat currency in and out of BTC-e. BTC-e's own website stated it was located in Bulgaria, yet simultaneously stated it was subject to the laws of Cyprus. Meanwhile, BTC-e's managing shell company, CANTON BUSINESS CORPORATION, was based in the Seychelles but affiliated with a Russian phone number, and its web domains were registered to shell companies in countries including Singapore, the British Virgin Islands, France, and New Zealand.

BACKGROUND

9. Bitcoin is a form of decentralized, convertible digital currency that existed through the use of an online, decentralized ledger system.[2] Bitcoin is just one of many forms of digital currency. There are many others, including litecoin, ethers, worldcoin, and dogecoin. However, bitcoin has the largest market capitalization of any present form of decentralized digital currency.

10. While bitcoin mainly exists as an Internet-based form of currency, it is possible to "print out" the necessary information and exchange bitcoin via physical medium. The currency is not issued

[2] Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use "Bitcoin" (singular with an uppercase letter B) to label the protocol, software, and community, and "bitcoin" (with a lowercase letter b) to label units of the currency. That practice is adopted here.

by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire bitcoin, a typical user will purchase them from a Bitcoin seller or "exchanger." It is also possible to "mine" bitcoin by verifying other users' transactions. Bitcoin is just one form of digital currency, and there are a significant number of other varieties of digital currency.

11. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value from government regulation or law), or other convertible digital currencies. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or ACH, or other convertible digital currency to an exchanger, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will then typically attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself. If the exchanger can place a buyer with a seller, then the transaction can be completed.

12. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user's bitcoin address. The bitcoin address is somewhat analogous to a bank account number, and is comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can then conduct transactions with other Bitcoin users, by transferring bitcoin to their bitcoin addresses, via the Internet.

13. Little to no personally identifiable information about the payer or payee is transmitted in a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address. Only the bitcoin address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any identifying information.

14. All bitcoin transactions are recorded on what is known as the blockchain. This is essentially a distributed public ledger that keeps track of all bitcoin transactions, incoming and outgoing, and updates approximately six times per hour. The blockchain records every bitcoin address that has ever received a bitcoin and maintains records of every transaction for each bitcoin address.

15. Digital currencies, including bitcoin, have many known legitimate uses. However, much

like cash, bitcoin can be used to facilitate illicit transactions and to launder criminal proceeds, given the ease with which bitcoin can be used to move funds with high levels of anonymity. As is demonstrated herein, however, in some circumstances bitcoin payments may be effectively traced by analyzing the blockchain.

BTC-E OVERVIEW

16. BTC-e was founded in or about 2011. In the years it operated, BTC-e has served approximately 700,000 users worldwide, including numerous customers in the United States and customers in the Northern District of California. BTC-e touts itself as "a platform for individuals interested in buying and selling bitcoin using an assortment of world currencies;" in other words, a digital currency exchange.

17. Through the work of VINNIK and others known and unknown to the Grand Jury, BTC-e became one of the primary ways by which cybercriminals around the world transferred, laundered, and stored the criminal proceeds of their illegal activities. U.S. dollars and Russian rubles were the most frequently exchanged fiat currencies on the platform, while Bitcoin and litecoin were the most widely exchanged digital currencies.

18. Because such a significant portion of BTC-e's business was derived from suspected criminal activity and given its global reach, the scope of the defendants' unlawful conduct was massive. During the relevant timeframe from 2011 to December 30, 2016, bitcoin addresses associated with BTC-e had received over 9.4 million bitcoin. Bitcoin's rapidly fluctuating exchange rate makes it difficult to determine the U.S. Dollar value of this quantity of bitcoin over time. However, using today's bitcoin exchange rate, the total value of bitcoin received by BTC-e over the course of its operation would be valued at over $9 billion. In 2016 alone, BTC-e received over 1.8 million bitcoin, valued at over $1.7 billion at today's exchange rate.[3]

[3] This is calculated using the December 30, 2016 bitcoin trading value of approximately $962 per bitcoin. Since August 2011, the Bitcoin market price has fluctuated from a low of roughly $2 to a high

19. Notably, the above figures only include bitcoin exchanged on the BTC-e platform and do not even include the deposits and withdrawals made in other digital currencies, such as litecoin, nor do these figures take into account well over a billion dollars' worth of what is known as "BTC-e code." BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other BTC-e users.

20. BTC-e maintained its servers in the United States. The servers were one of the primary ways in which BTC-e and the defendants effectuated their operations. BTC-e also used many third-party companies, including companies within the Northern District of California, to effectuate their operations and enable them to function.

21. At its inception, BTC-e was one of a number of digital currency exchanges. It was engaged in the same line of business as other online digital currency exchanges in existence at the time, including Liberty Reserve. Liberty Reserve was a Costa Rica-based centralized digital currency service that laundered approximately $6 billion in criminal proceeds. It was shuttered in 2013 when its founder and six other individuals were charged with conspiracy to commit money laundering and with operating an unlicensed money transmitting business. Liberty Reserve's website was seized by the U.S. government.[4]

22. There was an overlap between many Liberty Reserve users and BTC-e users. BTC-e itself was a user of Liberty Reserve.

23. Another digital currency exchange in operation between 2011 and 2014 was the MTGOX Exchange ("Mt. Gox") that was originally founded in San Francisco, but ultimately based in Tokyo, Japan. In 2014, Mt. Gox collapsed, having been the target of a series of major intrusions that resulted in thefts totaling several hundred million dollars worth of bitcoin. In 2014, Mt. Gox filed for bankruptcy in

---

of approximately $1200 per bitcoin and has varied dramatically over time..

[redacted]

Japan.

24. After the collapse of Liberty Reserve, and with the intrusions and accompanying issues that Mt. Gox experienced, BTC-e rapidly grew. The volume of transactions it performed and its number of users expanded, filling the vacuum left by entities like Liberty Reserve and Mt. Gox.

ENTITIES AND INDIVIDUALS

[redacted]

29. CANTON BUSINESS CORPORATION ("CANTON") was a shell corporation used as a

front for BTC-e's operations. Like BTC-e, CANTON was not registered with FinCEN. Financial and other records demonstrate that CANTON was synonymous with BTC-e. VINNIK, a Russian national, was a primary beneficial owner of CANTON's financial accounts. Although CANTON's listed business address was in the Seychelles, it operated using a Russian telephone number.

30. VINNIK also operated and controlled multiple BTC-e accounts, including a BTC-e account known as the "WME" account. The "WME" account was tied directly to BTC-e administrator accounts. Numerous withdrawals from BTC-e administrator accounts went directly to bank accounts tied to VINNIK.

31. Another such administrator account associated with VINNIK was the "Vamnedam"[5] account. The "Vamnedam" account was directly linked to the BTC-e administrative, financial, operational and support accounts, accounts to which only those involved in the operations of the BTC-e enterprise would have had access. Proceeds from well-known hacks and thefts from bitcoin exchanges and users around the world funded the Vamnedam account. Out of the Vamnedam account, large payments were made to accounts associated with VINNIK and others known and unknown to the Grand Jury, including a Russian national hereafter referred to as unindicted CO-CONSPIRATOR X, who is alleged to have access to the Vamnedam account.

BTC-E FUNCTION

32. To use BTC-e, one created an account by accessing the BTC-e website. A user did not need to provide even the most basic identifying information such as name, date of birth, address, or other identifiers. All that BTC-e required was a username, password, and an email address. Unlike legitimate payment processors or digital currency exchangers, BTC-e did not require its users to validate their identity information by providing official identification documents, given that BTC-e did not require an identity at all.

[5] Vamnedam means "I will not give it to you" in Russian.

33. Thus, a user could create a BTC-e account with nothing more than a username and email address, which often bore no relationship to the identity of the actual user. Accounts were therefore easily opened anonymously, including by customers in the United States within the Northern District of California.

34. At all times relevant to this Indictment, BTC-e had no anti-money laundering and/or "Know-Your-Customer" (KYC) processes and policies in place. As discussed above, BTC-e collected virtually no customer data at all. Nor did BTC-e or its shell companies ever register with FinCEN or perform these functions on BTC-e's behalf.

35. A user could fund a BTC-e account in numerous different ways. One way involved funding the account with fiat currency that would be converted into digital currency, such as bitcoin. With fiat currency, a user could initiate a wire transfer from a financial institution made directly for the benefit of BTC-e to an account at another financial institution, which was routed to a bank account maintained by one of BTC-e's shell or affiliated companies. [redacted]

36. Another way involved funding a BTC-e account with a user's existing digital currency. A user with existing digital currency, such as bitcoin, could fund a BTC-e account directly via bitcoin deposits. BTC-e users could also purchase "BTC-e code" that could be sent and exchanged amongst BTC-e users. BTC-e code enabled a BTC-e user to send and/or receive fiat currencies and digital currencies to other BTC-e users. This served as another conduit for money laundering as it allowed BTC-e customers to withdraw funds from their BTC-e account and transfer them to other BTC-e users

anonymously.

37. BTC-e's business model obscured and anonymized transactions and source of funds. For example, a BTC-e user could not fund an account by directly transferring money to BTC-e itself, but rather had to wire funds to one of BTC-e's shells or affiliate entities. Nor could BTC-e users withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were required to make any deposits or withdrawals through the use of third-party "exchangers," thus enabling BTC-e to avoid collecting any information about its users through banking transactions or other activity that would leave a centralized financial paper trail.

38. Once a user funded an account with BTC-e, the user could then do any number of things: conduct transactions with other BTC-e users; exchange digital currency into fiat currency; or simply use BTC-e to store digital currency deposits, much like a bank.

39. Like other digital currency exchanges, BTC-e charged transaction fees for their services. BTC-e charged a percentage fee every time a user transferred funds held in BTC-e to another user through the BTC-e system. In addition, BTC-e charged a percentage fee every time a user used BTC-e to exchange digital currency held in a BTC-e account into fiat currency.[6]

40. In addition to the fees BTC-e charged, users were charged additional fees by [redacted] each taking a percentage of the funds exchanged. These added fees were associated with getting money in and out of the BTC-e platform through these funding mechanisms, mechanisms that obfuscated the true sender of the currency.

41. Those engaged in criminal activity using BTC-e gravitated to BTC-e because of the site's lack of anti-money laundering and "Know-Your-Customer" processes in place that could have them reported to the government. Criminals who used BTC-e to launder funds were also willing to go to the extra trouble of wiring money offshore to entities that operated through shell companies.

[redacted]

42. BTC-e made a series of self-serving public statements, designed at least in part to deflect the attention of law enforcement and regulators. For example, despite advertising on their website that "[w]e require our clients to verify identity by providing [sic] scanned copy of ID and scanned copy of utility bill or a bank statement which should not be older then [sic] 6 month. Copy should be in good resolution and colored," this process was not in fact followed. As discussed, no customer identification whatsoever was required to set up BTC-e accounts, including BTC-e accounts set up by customers in the Northern District of California.

43. Likewise, the BTC-e website advertised that "[w]e don't accept any more international wire transfers from US Citizens or from US Bank." This, too, was false. Through its elaborate funding mechanisms, BTC-e did in fact knowingly accept wire transfers from banks in the U.S. and made by U.S. citizens.

BTC-E'S CRIMINAL DESIGN

44. As described above, BTC-e's system was designed so that criminals could accomplish financial transactions with anonymity and thereby avoid apprehension by law enforcement or seizure of funds. BTC-e was in fact thus used extensively for illegal purposes, and, particularly since the collapse of entities like Mt. Gox and Liberty Reserve, it functioned as the exchange of choice to convert digital currency like bitcoin to fiat currency for the criminal world, especially by those who committed their crimes online.

45. The defendants were aware that BTC-e functioned as a money laundering enterprise. Messages on its own forum openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged, and how they used BTC-e to launder funds.

46. BTC-e users established accounts under monikers suggestive of criminality, including monikers such as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire."

47. This is not surprising because criminals used BTC-e to launder criminal proceeds and

transfer funds among criminal associates. In particular, it was used by hacking and computer intrusion rings operating around the world to distribute criminal proceeds of their endeavors. It was also used by rings of identity thieves, corrupt public officials, narcotics distribution networks, and other criminals.

48. In fact, some of the largest known purveyors of ransomware used BTC-e as a means of storing, distributing, and laundering their criminal proceeds. Ransomware is a criminal scheme in which cybercriminals orchestrate the unwanted malicious download of encryption software on an unsuspecting victim computer. It works as follows: once a victim is infected with the malicious software, often by clicking on a fraudulent email, the ransomware will encrypt multiple files types on victim machines and hold those files for ransom, requiring the victim to pay the administrators of the ransomware scheme in order to have their files decrypted. Victims that pay the ransom are able to decrypt their files by using a stand-alone program provided by the ransomware administrators after the ransom payment has been made. The method of encryption implemented by the ransomware, if properly executed, renders it impossible for victims to decrypt their encrypted files in any other way. The most prevalent payment method accepted by current purveyors of ransomware is bitcoin.

49. One such ransomware scheme, CryptoWall, was distributed by methods including fraudulent and phishing emails. CryptoWall was one of the most infamous varieties of ransomware and has infected a vast number of computers across the world. During the timeframe relevant to this Indictment, the purveyors of CryptoWall deposited and laundered many hundreds of thousands of dollars' worth of ransom payments into BTC-e.

50. So, too, did a pair of corrupt U.S. federal agents, Carl Mark Force and Shaun Bridges, use BTC-e to launder their criminal proceeds. Their experience with the criminal underworld taught them that using BTC-e, as opposed to a registered exchange with anti-money laundering policies, would maximize their chances of being able to conceal criminal proceeds. Each therefore sent several hundred thousand dollars in criminal proceeds – derived from crimes ranging from theft of government property

to extortion – to the BTC-e platform for laundering.

51. BTC-e also served as the receptacle and transmitter of criminal funds from a series of well-publicized computer intrusions and resulting thefts, including the well-publicized thefts from the Japan-based Mt. Gox exchange. As discussed below, a sizable portion of the stolen Mt. Gox funds were deposited into accounts controlled, owned, and operated by BTC-e and by defendant VINNIK and others known and unknown to the Grand Jury.

52. The Mt. Gox exchange was the subject of a series of computer intrusions and resulting thefts between approximately September 2011 and May 2014, in violation of Title 18, United States Code, Section1030(a)(4). Several hundred millions dollars' worth of bitcoin was stolen, including from numerous customers in the U.S. and within the Northern District of California. After the thefts, some approximately 530,000 of the bitcoin (worth hundreds of millions of dollars) stolen from Mt. Gox was deposited into wallets at three different digital currency exchanges: (i) BTC-e; (ii) Trade Hill, another exchange based in San Francisco; and (iii) back into Mt. Gox into a different Mt. Gox wallet.

53. Of this 530,000 bitcoin,[7] 300,000 of it was sent directly to three separate BTC-e accounts: "Vamnedam," "Grmbit," and "Petr." These accounts were all linked to each other.

54. Meanwhile, blockchain analysis reveals that the stolen Mt. Gox funds that went to Trade Hill and back into the other Mt. Gox account were controlled by a user who also controlled a BTC-e account called "WME." At all times relevant to this Indictment, defendant VINNIK exercised control over the BTC-e "WME" account.

55. The "Vamnedam," "Grmbit," "Petr," and "WME" accounts were each directly linked to a variety of different BTC-e administrative accounts, accounts for which only BTC-e administrators and/or operators would have had access. The "Vamnedam" account was similarly a

[7] The amount of bitcoin stolen from Mt. Gox accounted for just under half of the total thefts that Mt. Gox suffered.

56. VINNIK, along with others known and unknown, controlled and operated the "Vamnedam" account. Between approximately August 2013 and November 2015, CO-CONSPIRATOR X and identities linked to VINNIK and to BTC-e received direct payments from the "Vamnedam" account to their own personal digital currency accounts at another digital currency exchange, Bitstamp. These bitcoin were then exchanged into fiat currency and sent to bank accounts in Cyprus and Latvia tied to VINNIK and other identities associated with VINNIK and BTC-e.

STATUTORY ALLEGATIONS

COUNT ONE: (18 U.S.C. § 1960 – Operation of an Unlicensed Money Transmitting Business)

57. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein as if set forth in full.

58. Title 18, United States Code, Section 1960, makes it a crime to operate an unlicensed money transmitting business. The term money transmitting includes "transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier." This statute makes it a violation to conduct a "money transmitting business" if the business is not registered as a money transmitting business with the Secretary of the Treasury as required by a separate statute, Title 31, United States Code, Section 5330 and federal regulations pursuant to that statute.

59. The regulations specifically apply to foreign-based money transmitting businesses doing substantial business in the United States. See C.F.R. §§ 1010.100(ff)(5), 1022.380(a)(2).

60. From in or about 2011, up to and including in or about May 2016, both dates being approximate and inclusive, in the Northern District of California and elsewhere, the defendants,

BTC-e a/k/a CANTON BUSINESS CORPORATION, and
ALEXANDER VINNIK,

and others known and unknown to the Grand Jury, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of a money transmitting business affecting interstate and foreign commerce, i.e. BTC-e, which (i) failed to comply with the money transmitting business

registration requirements set forth in Title 31, United States Code, Section 5330, and the regulations prescribed pursuant to that statute, including 31 C.F.R. Sections 1010.100(ff) (5) and 1022.380(a)(2); and (ii) otherwise involved the transportation and transmission of funds known to the defendants to have been derived from a criminal offense and intended to be used to promote and support unlawful activity.

All in violation of Title 18, United States Code, Sections 1960 & 2.

COUNT TWO: (18 U.S.C. § 1956(h) – Conspiracy to Commit Money Laundering)

61. The factual allegations in paragraphs 1 through 60 are re-alleged and incorporated herein as if set forth in full.

62. From in or about July 2011, through in or about January 2017, both dates being approximate and inclusive, within the Northern District of California, and elsewhere, the defendants;

BTC-e a/k/a CANTON BUSINESS CORPORATION, and
ALEXANDER VINNIK,

and others known and unknown to the Grand Jury, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, operation of an unregistered money transmitting business in violation of Title 18, United States Code, Sections 1960: computer hacking and intrusions in violation of Title 18, United States Code, Section 1030; identity theft in violation of Title 18, United States Code, Section 1028; interstate transportation of stolen property in violation of Title 18, United States Code, Section 2314; theft of government proceeds and extortion in violation of Title 18, United States Code, Sections 641 and 1951; and narcotics trafficking in violation of Title 21, United States Code, Section 841; with the intent to promote the carrying on of the specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i).

All in violation of Title 18, United States Code, Section 1956(h).

COUNTS THREE THROUGH NINETEEN: (18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i) – Money Laundering)

On or about the dates described below, in the Northern District of California and elsewhere, the defendant,

ALEXANDER VINNIK,

aided and abetted by others, known and unknown to the Grand Jury, did knowingly conduct and attempt to conduct the listed financial transactions affecting interstate and foreign commerce which involved the proceeds of a specified unlawful activity, that is accessing a computer in furtherance of fraud, in violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A), with the intent to promote the carrying on of said specified unlawful activity, and knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and proceeds of said specified unlawful activity, and that while conducting and attempting to conduct such financial transaction, knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity.

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
THREE	01/23/2012	90 BTC	$567.00	Transfer of BTC into Tradehill
FOUR	01/23/2012	83 BTC	$522.07	Transfer of BTC into Tradehill
FIVE	01/23/2012	61 BTC	$383.69	Transfer of BTC into Tradehill
SIX	01/24/2012	91 BTC	$573.30	Transfer of BTC into Tradehill
SEVEN	01/24/2012	90 BTC	$567.00	Transfer of BTC into Tradehill
EIGHT	01/24/2012	99 BTC	$623.70	Transfer of BTC into Tradehill
NINE	01/24/2012	533 BTC	$3,357.90	Transfer of BTC into Tradehill
TEN	01/24/2012	1900 BTC	$11,970.00	Transfer of BTC into Tradehill
ELEVEN	01/24/2012	579 BTC	$3,647.70	Transfer of BTC into Tradehill
TWELVE	01/24/2012	2 BTC	$12.60	Transfer of BTC into Tradehill
THIRTEEN	01/27/2012	1000 BTC	$5,290.00	Transfer of BTC into Tradehill
FOURTEEN	01/27/2012	1500 BTC	$7,935.00	Transfer of BTC into Tradehill
FIFTEEN	02/01/2012	1000 BTC	$5,820.00	Transfer of BTC into Tradehill
SIXTEEN	02/01/2012	1000 BTC	$5,820.00	Transfer of BTC into Tradehill
SEVENTEEN	02/05/2012	3000 BTC	$17,040.00	Transfer of BTC into Tradehill
EIGHTEEN	02/05/2012	500 BTC	$2,840.00	Transfer of BTC into Tradehill
NINETEEN	02/12/2012	2000 BTC	$11,200.00	Transfer of BTC into Tradehill

All in violation of Title 18, United States Code, Sections 1956(a)(1)(A)(i), (a)(1)(B)(i), and 2.

COUNTS TWENTY THROUGH TWENTY-ONE: (18 U.S.C. § 1957 – Engaging in Unlawful Monetary Transactions)

On or about the dates described below, in the Northern District of California and elsewhere, the defendant,

ALEXANDER VINNIK,

aided and abetted by others, known and unknown to the Grand Jury, did knowingly engage and attempt to engage in the listed monetary transactions by through or to a financial institution affecting interstate and foreign commerce in criminally derived property of a value greater than $10,000, that is the transactions listed below, such property having been derived from a specified unlawful activity, that is accessing a computer in furtherance of fraud, in violation of Title 18, United States Code, Section 1030(a)(4) and (c)(3)(A).

COUNT	DATE	AMOUNT (BTC)	AMOUNT (USD)	TRANSACTION
TWENTY	02/05/2012	3000 BTC	$17,040.00	Transfer of BTC into Tradehill
TWENTY-ONE	02/12/2012	2000 BTC	$11,200.00	Transfer of BTC into Tradehill

All in violation of Title 18, United States Code, Sections 1957 and 2.

FORFEITURE ALLEGATION: (18 U.S.C. §§ 982(a)(1) – Criminal Forfeiture)

63. All of the allegations contained in this Indictment are re-alleged and by this reference fully incorporated herein for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Section 982(a)(1).

64. Upon a conviction for any of the offenses alleged in this Indictment, the defendants,

BTC-e a/k/a CANTON BUSINESS CORPORATION, and
ALEXANDER VINNIK,

shall forfeit to the United States pursuant to 18 U.S.C. § 982(a)(1) any property, real or personal, involved in those offenses or any property traceable to such offenses including but not limited to a forfeiture money judgment.

If any of the aforementioned property, as a result of any act or omission of the defendants

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property that cannot be divided without difficulty;

any and all interest the defendant has in other property shall be vested in the United States and forfeited to the United States pursuant to 21 U.S.C. § 853(p), as incorporated by 18 U.S.C. § 982(b)(1).

All in violation of Title 18, United States Code, Section 982(a)(1) and Rule 32.2 of the Federal Rules of Criminal Procedure.

DATED: 1/17/17

A TRUE BILL

FOREPERSON

BRIAN J. STRETCH
United States Attorney

BARBARA J. VALLIERE
Chief, Criminal Division

(Approved as to form:

WILLIAM FRENTZEN
KATHRYN HAUN
Assistant U.S. Attorneys

SEALED BY COURT ORDER

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CRIMINAL COVER SHEET

Instructions: Effective November 1, 2016, this Criminal Cover Sheet must be completed and submitted, along with the Defendant Information Form, for each new criminal case.

CASE NAME: USA v.	**BTC-E a/k/a Canton Business Corporation and Alexander Vinnik**	**CASE NUMBER:**	**CR 16-00227 SI**
Is This Case Under Seal?	**Yes** ✓	**No**	
Total Number of Defendants:	**1**	**2-7** ✓	**8 or more**
Does this case involve ONLY charges under 8 U.S.C. § 1325 and/or 1326?	**Yes**	**No** ✓	
Venue (Per Crim. L.R. 18-1):	**SF** ✓	**OAK**	**SJ**
Is this a potential high-cost case?	**Yes**	**No** ✓	
Is any defendant charged with a death-penalty-eligible crime?	**Yes**	**No** ✓	
Is this a RICO Act gang case?	**Yes**	**No** ✓	

Assigned AUSA (Lead Attorney): William Frentzen **Date Submitted:** 01/17/2017

Comments:

RESET FORM SAVE PDF

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SERVERS CONTAINING BTC-E-RELATED CONTENT STORED AT THE PREMISES CONTROLLED BY EQUINIX	**Mag. No. 17-8128** **Leda Dunn Wettre** **SEALING ORDER**

This matter having been brought before the Court upon application of William E. Fitzpatrick, Acting United States Attorney for the District of New Jersey (Jason S. Gould, Assistant United States Attorney, appearing), for an order sealing the search warrant issued on this date and the application and attached Affidavit in support of that warrant, and for good cause shown,

IT IS on this 21st Day of July 2017,

ORDERED that the search warrant, the application and affidavit in support of the search warrant, and all related documents, except for one copy of the search warrant and inventory to be served at the time the search is executed, be and hereby are sealed until further Order of this Court.

Leda Dunn Wettre

Hon. Leda Dunn Wettre
United States Magistrate Judge

EXHIBIT B

DAVID L. ANDERSON (CABN 149604)
United States Attorney

SARA WINSLOW (DCBN 457643)
Chief, Civil Division

KIRSTIN M. AULT (CABN 206052)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-6940
FAX: (415) 436-7234
Kirstin.ault@usdoj.gov

Attorneys for United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-e, a/k/a CANTON BUSINESS CORP., and ALEXANDER VINNIK, Defendants.	CASE NO. **COMPLAINT**

The United States of America alleges as follows:

I. NATURE OF ACTION

1. The United States brings this action against BTC-e a/k/a Canton Business Corporation ("BTC-e") and Alexander Vinnik ("Vinnik") (collectively "Defendants"), to recover civil money penalties imposed under the Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. §§ 5311-5314 and 5316-5332, which is commonly referred to as the Bank Secrecy Act ("BSA").

II. JURISDICTION AND VENUE

2. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1345. The Court may exercise personal jurisdiction over Defendants because they transact business in this District.

3. Venue is proper in the Northern District of California under 28 U.S.C. §§ 1391(b) and (c) because Defendants transact business in this District.

III. PARTIES

4. The United States brings this action on behalf of the Department of the Treasury.

5. Defendant BTC-e is a corporation organized under the laws of either Cyprus and/or the Seychelles Islands. BTC-e operated in Bulgaria, the Seychelles Islands, and other jurisdictions, including the Northern District of California. At all times relevant to this complaint, BTC-e was a money services business providing services subject to the BSA in the Northern District of California and elsewhere.

6. Defendant Alexander Vinnik is a Russian national who is currently incarcerated in Greece. At all times relevant to this complaint, Vinnik occupied a senior leadership position within BTC-e.

IV. THE BANK SECRECY ACT

7. The Financial Crimes Enforcement Network ("FinCEN"), a bureau within the United States Department of the Treasury, administers the BSA pursuant to authority delegated by the Secretary of the Treasury. *See* Treasury Order 180-01 (July 1, 2014). The BSA requires the filing of reports and the maintenance of records useful in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism.

Regulations implementing the BSA appear at 31 C.F.R. Chapter X. Rules issued under the BSA require the registration of money services businesses ("MSBs"), the filing of Suspicious Activity Reports ("SARs"), the implementation of anti-money laundering ("AML") programs, and the maintenance of records related to transmittals of funds.

8. FinCEN may impose a civil monetary penalty "at any time before the end of the 6-year period beginning on the date of the transaction with respect to which the penalty was assessed," and may commence an action to recover the civil money penalty at any time before the end of the 2-year period beginning on the date the penalty was imposed. *See* 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

9. MSBs are "financial institutions" for purposes of the BSA and its implementing regulations. *See* 31 U.S.C. § 5312(a)(2)(J), (K) and (R); 31 C.F.R. § 1010.100(t)(3). A "money services business" is defined in regulations implementing the BSA to include persons who are engaged as a business in providing money transmission services "wholly or in substantial part within the United States." *See* 31 C.F.R. § 1010.100(ff)(5). Exchangers of convertible virtual currency provide "money transmission services" for purposes of regulations implementing the BSA and may therefore qualify as MSBs. *See* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies" (March 18, 2013).

10. FinCEN may impose on any person who owns or controls an unregistered MSB a civil money penalty for each day that the MSB remains unregistered. *See* 31 U.S.C. § 5330(e)(2); 31 C.F.R. § 1022.380(e). For MSB registration violations occurring on or before November 2, 2015, FinCEN may assess a penalty of up to $7,954 for each violation. 31 C.F.R. § 1010.821. Violations occurring after November 2, 2015, may be assessed in an amount up to $8,084 for each violation. *Id*. Each day a violation continues constitutes a separate violation. 31 C.F.R. § 1022.380(e).

11. FinCEN may impose a civil money penalty on a domestic financial institution that willfully violates the BSA by failing to establish or maintain an adequate AML program and for failing to file SARs as appropriate, and on any partner, director, officer or employee who willfully participates in the violation. *See* 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820. The term "domestic" refers to "the doing of business within the United States" or the performance of functions within the United States. 31 C.F.R. § 1010.100(o); *see also* 31 U.S.C. § 5312(b)(1). For violations occurring on or before November

2, 2015, FinCEN may impose a penalty of $25,000 to $100,000 for willful violations of BSA program requirements. 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f). For AML program violations after November 2, 2015, FinCEN may impose a penalty of $54,789 to $219,156. 31 C.F.R. § 1010.821. For violations of the requirement to implement an adequate AML program, "a separate violation occurs for each day that the violation continues." *See* 31 U.S.C. § 5321(a)(1) and 31 C.F.R. §1010.821.

V. FACTUAL ALLEGATIONS

A. Bitcoin and Digital Currencies

12. Bitcoin is a form of decentralized, convertible digital currency that exists through the use of an online, decentralized ledger system. Bitcoin is just one of many forms of digital currency. There are many others, including litecoin, ether, worldcoin, and dogecoin; however, bitcoin has the largest market capitalization of any present form of decentralized digital currency. While bitcoin is an internet-based form of currency, it is possible to "print out" the necessary bitcoin information and exchange it via physical media. Bitcoin is not issued by any government, bank, or company, but rather is generated and controlled through computer software operating via a decentralized network. To acquire bitcoin, a typical user will purchase it from a bitcoin seller or "exchanger."

13. Bitcoin exchangers typically accept payments of fiat currency (currency which derives its value from government regulation or law), or other convertible digital currencies. When a user wishes to purchase bitcoin from an exchanger, the user will typically send payment in the form of fiat currency, often via bank wire or automated clearing house ("ACH") transfer, for the corresponding quantity of bitcoin, based on a fluctuating exchange rate. The exchanger, often for a commission, will then attempt to broker the purchase with another user of the exchange that is trying to sell bitcoin, or, in some instances, will act as the seller itself.

14. When a user acquires bitcoin, ownership of the bitcoin is transferred to the user's bitcoin address. The bitcoin address is somewhat analogous to a bank account number and is comprised of a case-sensitive string of letters and numbers amounting to a total of 26 to 35 characters. The user can then conduct transactions with other bitcoin users by transferring bitcoin to their bitcoin addresses via the internet.

15. Little to no personally identifiable information about the payer or payee is transmitted in

a bitcoin transaction itself. Bitcoin transactions occur using a public key and a private key. A public key is used to receive bitcoin, and a private key is used to allow withdrawals from a bitcoin address. Only the bitcoin address of the receiving party and the sender's private key are needed to complete the transaction. These two keys by themselves rarely reflect any information identifying the payer or payee.

16. All bitcoin transactions are recorded on what is known as the Blockchain. The Blockchain is a distributed public ledger that maintains all bitcoin transactions, incoming and outgoing. The Blockchain records every bitcoin address that has ever received a bitcoin and maintains records of every transaction for each bitcoin address. In some circumstances, bitcoin payments may be effectively traced by analyzing the Blockchain.

B. BTC-e Operations

17. BTC-e was a digital currency exchange that allowed users to buy and sell bitcoin, and other digital currencies, anonymously through its web domain btc-e.com. Since its founding, BTC-e has served approximately 700,000 users worldwide, including numerous customers in the United States and in the Northern District of California. BTC-e was used by cybercriminals worldwide and was one of the principal entities used to launder and liquidate criminal proceeds, converting them from digital currencies, including bitcoin, to fiat currencies, including U.S. Dollars, Euros, and Rubles.

18. To use BTC-e, a user created an account by accessing BTC-e's website, www.btc-e.com. To create an account, a user did not need to provide even the most basic identifying information, such as name, date of birth, address, or other identifiers. All BTC-e required to create a user account was a self-created username, password, and an email address. Unlike legitimate digital currency exchangers, BTC-e did not require its users to validate their identity by providing official identification documents. When a customer attempted to use bank wires to transfer funds to or from BTC-e's exchange, BTC-e at times did request identifying documentation, such as a driver's license or passport. BTC-e did not request such documents for all transactions involving bank wires or for other types of transactions.

19. BTC-e's business model obscured and anonymized transactions and sources of funds. A BTC-e user did not fund an account by directly transferring money to BTC-e itself, but rather users were instructed to wire funds to one of BTC-e's "front" companies that, although nominally separate from BTC-e were, in fact, controlled by and operated for the benefit of BTC-e. Nor could BTC-e users

withdraw funds from their accounts directly, such as through an ATM withdrawal. Instead, BTC-e users were required to make withdrawals through the use of third-party "exchangers" or other processors, thus enabling BTC-e to avoid collecting any information about its users that would leave a centralized financial paper trail. Thus, a user could create a BTC-e account with nothing more than a username and email address, which often bore no relationship to the actual identity of the user.

20. BTC-e accounts received criminal proceeds directly from various cybercrimes, including numerous hacking incidents, ransomware payments, identity theft schemes, embezzlement by corrupt public officials, and narcotics distribution. A significant portion of BTC-e's business was derived from suspected criminal activity.

21. Messages on BTC-e's own forum openly and explicitly reflected some of the criminal activity in which the users on the platform were engaged and how they used BTC-e to launder funds. BTC-e users established accounts under monikers suggestive of criminality, including user names such as "ISIS," "CocaineCowboys," "blackhathackers," "dzkillerhacker," and "hacker4hire." Despite these suspicious usernames, BTC-e did nothing to identify these customers or to investigate whether these or any of its other customers were using its services to conduct, conceal, or facilitate illegal activity.

22. BTC-e's structure allowed criminals to conduct financial transactions with high levels of anonymity and thereby avoid apprehension by law enforcement or seizure of funds. This aspect of BTC-e contributed to its customers' willingness to accept BTC-e's unfavorable exchange rates compared to other legitimate digital currency exchangers that registered with FinCEN and that had appropriate and effective anti-money laundering and "Know-Your-Customer" policies in place.

23. Customers located within the United States used BTC-e to conduct at least 21,000 bitcoin transactions worth over $296,000,000 and tens of thousands of transactions in other convertible virtual currencies.

24. BTC-e made no effort to register with FinCEN, maintain any elements of an AML program, or report suspicious activity.

C. Vinnik

25. Vinnik occupied a senior leadership position within BTC-e and participated in the direction and supervision of BTC-e's operations and finances. Vinnik controlled multiple BTC-e

administrative accounts used to process BTC-e's transactions.

26. The owners and administrators of BTC-e, including Vinnik, were aware BTC-e functioned as a money laundering enterprise. Vinnik sent emails claiming to be an owner of BTC-e and used the site to personally conduct transactions with illegal proceeds.

27. Vinnik operated several administrative, financial, operational, and support accounts at BTC-e, including accounts that have been tied to thefts from other virtual currency exchanges such as Mt. Gox. Furthermore, withdrawals from these accounts were deposited directly into bank accounts tied to Vinnik. These accounts granted Vinnik the ability to observe transactions coming to and leaving from BTC-e, as well as specific customer activity and profiles. Vinnik made no efforts to ensure that BTC-e registered with FinCEN, maintained any elements of an AML program, or reported suspicious transactions.

D. Indictment

28. On May 31, 2016, a grand jury sitting in the Northern District of California returned a two-count indictment charging BTC-e and Alexander Vinnik with operation of an Unlicensed Money Services Business, in violation of 18 U.S.C § 1960, and Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h).

29. On January 17, 2017, the grand jury issued a twenty-one count superseding indictment charging BTC-e and Vinnik with Operation of an Unlicensed Money Services Business, in violation of 18 U.S.C § 1960; Conspiracy to Commit Money Laundering, in violation of 18 U.S.C. § 1956(h); Money Laundering, in violation of 18 U.S.C. § 1956(a)(1)(A)(i) and (a)(1)(B)(i); and Engaging in Unlawful Monetary Transactions, in violation of 18 U.S.C. § 1957.

E. FinCEN's Civil Monetary Penalty

30. As detailed in the Assessment of Civil Money Penalty issued on July 26, 2017 (attached hereto as Exhibit 1), FinCEN assessed monetary penalties against BTC-e and Vinnik for the following conduct:

<u>Failure to Register as an MSB</u>

31. A Money Services Business ("MSB") is any person or entity that receives something of value (including currency or value that substitutes for currency) from one person and transmits either the

same or a different form of value to another person or location by any means. 31 C.F.R. §1010.100(ff); 2011 MSB Final Rule, 76 FR 43585, at 43596. An MSB is required to register with FinCEN within 180 days of beginning operation and to renew such registration every two years. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(b)(2). Foreign-located MSBs that conduct business within the United States must register and must also appoint an agent within the United States to accept legal process in BSA-related matters. 31 U.S.C. § 5330; 31 C.F.R. § 1022.380(a)(2).

32. The BTC-e website (btc-e.com) Terms and Conditions contained the following information, "BTC-e provides an online tool that allows users to freely trade Bitcoins for a number of different currencies worldwide." Thus, BTC-e's business model was to transfer something of value – bitcoin and other cryptocurrency – between entities and individuals and between locations. As such, BTC-e was an MSB. At no point in its existence did BTC-e register as an MSB with FinCEN. In March of 2013, FinCEN issued guidance clarifying and affirming its July 2011 Final Rules establishing that exchangers and administrators that transmitted virtual currency and operated in the United States were subject to FinCEN requirements, including registration as an MSB. Nevertheless, BTC-e continued to fail to register.

Failure to Establish AML Programs and Procedures

33. Under the BSA, an MSB must develop, implement, and maintain an effective AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a). The AML program must: contain written policies, procedures and internal controls; designate an individual responsible for BSA compliance; provide training, including on how to detect suspicious transactions; and provide for independent review of the AML program. 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. §§ 1022.210(c) and (d).

34. At no point in time did BTC-e have any AML policies or procedures, let alone an effective program for detecting and preventing suspicious transactions. To the contrary, BTC-e's lax policies encouraged persons engaged in criminal activity to use its services, and BTC-e became the virtual currency exchange of choice for criminals looking to launder their illegal proceeds.

35. BTC-e had no policies or procedures to verify customer identification. BTC-e failed to

collect even the most basic customer information needed to comply with the BSA. BTC-e allowed its customers to open accounts and conduct transactions with only a username, password, and e-mail address. BTC-e collected only this limited information no matter how large the transaction or how many transactions the customer conducted. When BTC-e finally implemented policies to verify customer identification in May of 2017, it made those procedures "optional."

36. In fact, BTC-e processed digital currency transactions with features that restricted its ability to identify its customers and detect suspicious activity. For example, BTC-e processed millions of dollars' worth of transactions using bitcoin "mixers." Instead of transmitting bitcoin directly between two users, the "mixer" created layers of temporary bitcoin addresses operated by the mixer itself to complicate any attempt to analyze the flow of the transaction.

37. Moreover, BTC-e had no policies or procedures for conducting due diligence or monitoring transactions for suspicious activity. On some occasions, BTC-e customers contacted BTC-e's administration with questions regarding how to process and access proceeds obtained from the sale of illegal drugs and from transactions on known "darknet" illegal markets, including Silk Road. In addition, BTC-e's customers openly discussed using BTC-e to facilitate illegal activity on BTC-e's own internal messaging system, as well as on its public user chat system. Nevertheless, BTC-e did not implement any policies or procedures to monitor its platform for suspect activity.

Failure to File SARs

38. Under the BSA, an MSB must report transactions that the MSB "knows, suspects, or has reason to suspect" are suspicious where those transactions involve the MSB and aggregate to at least $2,000 in value. 31 U.S.C. § 5318(g)(1); 31 C.F.R. § 1022.320(a)(2). A transaction is "suspicious" if it (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or apparent lawful purpose; or (d) involves the use of the MSB to facilitate illegal activity. 31 U.S.C. § 5318(g)(1); 31 CFR. §§ 1022.320(a)(2)(i)-(iv).

39. Despite the rampant evidence of illegal activity on its platform, BTC-e did not file a single SAR, including for the specific activities identified in the Assessment.

40. On July 26, 2017, FinCEN imposed on BTC-e and Alexander Vinnik civil monetary penalties in the amounts of $88,596,314 and $12,000,000, respectively, for the conduct described above.

See Exhibit 1. Defendants have not paid the penalties.

FIRST CAUSE OF ACTION:
RECOVERY OF CIVIL MONETARY PENALTY

41. Plaintiff hereby incorporates by reference each and every allegation set forth in the foregoing paragraphs.

42. The July 26, 2017, Assessment of Civil Money Penalty constitutes a lawful administrative sanction against BTC-e and Vinnik for failure to comply with the BSA's requirements under 31 U.S.C. §§ 5321(b)(1) and 5330(e)(3).

43. BTC-e is liable to the United States for a civil penalty in the amount of $88,596,314, plus interest and costs.

44. Vinnik is liable to the United States for a civil penalty in the amount of $12,000,000, plus interest and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court reduce Plaintiff's claims against BTC-e and Alexander Vinnik to judgment, award Plaintiff judgments against BTC-e and Alexander Vinnik in the amounts of $88,596,314 and $12,000,000, respectively, plus interest as provided by law, and award such other relief as the Court deems just and proper, including Plaintiff's costs.

Dated: July 25, 2019

Respectfully submitted,

DAVID L. ANDERSON
United States Attorney

/s
KIRSTIN M. AULT
Assistant United States Attorney

Attorneys for United States of America

Exhibit 1

UNITED STATES OF AMERICA
DEPARTMENT OF THE TREASURY
FINANCIAL CRIMES ENFORCEMENT NETWORK

IN THE MATTER OF:	)	
	)	
	)	
	)	**Number 2017-03**
BTC-E a/k/a Canton Business Corporation and Alexander Vinnik	)	
	)	
	)	

ASSESSMENT OF CIVIL MONEY PENALTY

I. INTRODUCTION

The Financial Crimes Enforcement Network (FinCEN) has determined that grounds exist to assess civil money penalties against BTC-E a/k/a Canton Business Corporation (BTC-e) and Alexander Vinnik, pursuant to the Bank Secrecy Act (BSA) and regulations issued pursuant to that Act.[1]

FinCEN has the authority to impose civil money penalties on money services businesses (MSBs) and individuals involved in the ownership or operation of MSBs.[2] Rules implementing the BSA state that "[o]verall authority for enforcement and compliance, including coordination and direction of procedures and activities of all other agencies exercising delegated authority under this chapter" has been delegated by the Secretary of the Treasury to FinCEN.[3]

---

[1] The Bank Secrecy Act is codified at 12 U.S.C. §§ 1829b, 1951–1959 and 31 U.S.C. §§ 5311–5314, 5316–5332. Regulations implementing the Bank Secrecy Act currently appear at 31 C.F.R. Chapter X.

[2] 12 U.S.C. §§ 1829b(j) and 1955; 31 U.S.C. §§ 5321(a)(1) and 5330(e); 31 C.F.R. § 1010.820.

[3] 31 C.F.R. § 1010.810(a).

BTC-e and Alexander Vinnik have been indicted in the Northern District of California under 18 U.S.C. §§ 1956, 1957, and 1960 for money laundering, conspiracy to commit money laundering, engaging in unlawful monetary transactions, and the operation of an unlicensed money transmitting business.[4]

II. JURISDICTION

BTC-e operates as an "exchanger" of convertible virtual currencies, offering the purchase and sale of U.S. dollars, Russian Rubles, Euros, Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum, and Dash.[5] BTC-e also offered "BTC-e code," which enabled users to send and receive fiat currencies, including U.S. dollars, with other BTC-e users. Since 2011, BTC-e has served approximately 700,000 customers worldwide and is associated with bitcoin wallet addresses that have received over 9.4 million bitcoin. Alexander Vinnik participated in the direction and supervision of BTC-e's operations and finances and controlled multiple BTC-e administrative accounts used in processing transactions.

Exchangers of convertible virtual currency are "money transmitters" as defined at 31 C.F.R § 1010.100(ff)(5) and "financial institutions" as defined at 31 C.F.R § 1010.100(t). A foreign-located business qualifies as an MSB if it does business as an MSB "wholly or in substantial part within the United States."[6] Customers located within the United States used BTC-e to conduct at least 21,000 bitcoin transactions worth over $296,000,000 and tens of thousands of transactions in other convertible virtual currencies. The transactions included funds sent from customers located within the United States to recipients who were also located within the United States. In addition,

---

[4] *United States v. BTC-e a/k/a Canton Business Corporation and Alexander Vinnik*, CR 16-00227 SI (N.D. CA. Jan. 17, 2017).

[5] FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

[6] 31 U.S.C. §§ 5312(a)(6), 5312(b), and 5330(d); 31 C.F.R. § 1010.100(ff).

these transactions were processed through servers located in the United States. BTC-e attempted to conceal the fact that it provided services to customers located within the United States. BTC-e instructed customers to make use of correspondent accounts held by foreign financial institutions or services provided by affiliates of BTC-e located abroad.

III. DETERMINATIONS

FinCEN has determined that, from November 5, 2011 through the present: (a) BTC-e and Alexander Vinnik[7] willfully violated MSB registration requirements; (b) BTC-e willfully violated[8] the requirement to implement an effective anti-money laundering (AML) program, the requirement to detect suspicious transactions and file suspicious activity reports (SARs), and the requirement to obtain and retain records relating to transmittals of funds in amounts of $3,000 or more; and (c) Alexander Vinnik willfully participated[9] in violations of AML program and SAR requirements.[10]

A. Registration as a Money Services Business

The BSA and its implementing regulations require the registration of an MSB within 180 days of beginning operations and the renewal of such registration every two years.[11] A foreign-

[7] 31 U.S.C. § 5330(a)(1) ("Any person who owns or controls a money transmitting business shall register the business…"); 31 U.S.C. 5330(e)(1) ("Any person who fails to comply with any requirement of [31 U.S.C. § 5330] or any regulation prescribed under [31 U.S.C. § 5330] shall be liable…for a civil penalty…"); 31 C.F.R. § 1022.380(c) ("[A]ny person who owns or controls a money services business is responsible for registering the business…"); 31 C.F.R. § 1022.380(e) ("Any person who fails to comply with any requirement of [31 U.S.C. § 5330 or 31 C.F.R. § 1022.380] shall be liable for a civil penalty…").

[8] 12 U.S.C. § 1829b(j); 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f).

[9] 31 U.S.C. § 5321(a)(1); 31 C.F.R. § 1010.820(f) (For any willful violation…of any reporting requirement for financial institutions…, the Secretary may assess upon any domestic financial institution, and upon any partner, director, officer, or employee thereof who willfully participates in the violation, a civil penalty…).

[10] In civil enforcement of the Bank Secrecy Act under 31 U.S.C. § 5321(a)(1), to establish that a financial institution or individual acted willfully, the government need only show that the financial institution or individual acted with either reckless disregard or willful blindness. The government need not show that the entity or individual had knowledge that the conduct violated the Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose.

[11] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(b)(2).

located MSB must appoint an agent who will accept legal process in matters related to compliance with the BSA. [12] The agent must reside within the United States.

At no point in its operations was BTC-e registered with FinCEN. Notably, BTC-e went unregistered even after FinCEN issued guidance pertaining to exchangers and administrators of virtual currency in March 2013. BTC-e never appointed an agent for service of process.

B. Violations of AML Program Requirements

The BSA and its implementing regulations require an MSB to develop, implement, and maintain an effective written AML program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.[13] BTC-e was required to implement a written AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible to assure day to day compliance with the program and BSA requirements; (c) provides training for appropriate personnel, including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program.[14]

BTC-e lacked basic controls to prevent the use of its services for illicit purposes. Through their operation of BTC-e, Alexander Vinnik and other individuals occupying senior leadership positions within the virtual currency exchange attracted and maintained a customer base that consisted largely of criminals who desired to conceal proceeds from crimes such as ransomware, fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. BSA

---

[12] 31 U.S.C. § 5330 and 31 C.F.R. § 1022.380(a)(2). *See generally* FIN-2012-A001, "Foreign-Located Money Services Businesses," February 15, 2012.

[13] 31 U.S.C. §§ 5318(a)(2) and (h); 31 C.F.R. § 1022.210(a).

[14] 31 U.S.C. §§ 5318(a)(2) and (h)(1); 31 C.F.R. §§ 1022.210(c) and (d).

compliance was compromised by revenue interests. BTC-e quickly became the virtual currency exchange of choice for criminals looking to conduct illicit transactions or launder illicit proceeds, all of which BTC-e failed to report both to FinCEN and law enforcement.

1. Internal Controls

BTC-e failed to implement policies, procedures, and internal controls reasonably designed to prevent the MSB from facilitating money laundering. The BSA requires MSBs to implement policies and procedures to verify customer identification, file BSA reports, create and maintain BSA records, and respond to law enforcement requests. BTC-e lacked adequate controls to verify customer identification, to identify and report suspicious activity, and to prevent money laundering and the financing of terrorist activities. BTC-e offered a variety of convertible virtual currencies internationally and operated as one of the largest volume virtual currency exchanges. The BSA and its implementing regulations require an MSB to implement internal controls that are commensurate with the risks posed by its clientele, the nature and volume of the financial services it provides, and the jurisdictions in which the MSB provides its services.

BTC-e failed to collect and verify even the most basic customer information needed to comply with the BSA. BTC-e allowed its customers to open accounts and conduct transactions with only a username, password, and an email address. The minimal information collected was the same regardless of how many transactions were processed for a customer or the amount involved. BTC-e implemented policies to verify customer identification in May 2017 but stated that compliance with those policies was "optional."

BTC-e processed transactions with digital currency features that restricted its ability to verify customer identification or monitor for suspicious activity. BTC-e allowed over $40 million in transfers on its platform from bitcoin mixers. Mixers anonymize bitcoin addresses and obscure

bitcoin transactions by weaving together inflows and outflows from many different users. Instead of directly transmitting bitcoin between two bitcoin addresses, the mixer disassociates connections. Mixers create layers of temporary bitcoin addresses operated by the mixer itself to further complicate any attempt to analyze the flow of bitcoin. BTC-e lacked adequate internal controls to mitigate the risks presented by bitcoin mixers.

BTC-e also lacked adequate internal controls to mitigate the risks presented by virtual currencies with anonymizing features. BTC-e facilitated transfers of the convertible virtual currency Dash, which has a feature called "PrivateSend." PrivateSend provides a decentralized mixing service within the currency itself in an effort to enhance user anonymity. BTC-e and Alexander Vinnik failed to conduct appropriate risk-based due diligence to address the challenges anonymizing features would have on compliance with BSA reporting and recordkeeping requirements.

BTC-e lacked adequate procedures for conducting due diligence, monitoring transactions, and refusing to consummate transactions that facilitated money laundering or other illicit activity. Users of BTC-e openly and explicitly discussed conducting criminal activity through the website's internal messaging system and on BTC-e's public "Troll Box," or user chat. This resulted in no additional scrutiny from Alexander Vinnik or BTC-e's other operators and senior leadership. BTC-e received inquiries from customers on how to process and access proceeds obtained from the sale of illegal drugs on darknet markets, including Silk Road, Hansa Market, and AlphaBay.

BTC-e processed transactions involving funds stolen from the Mt.Gox exchange between 2011 and 2014. BTC-e processed over 300,000 bitcoin of these proceeds, which were sent and held at three separate but linked BTC-e accounts. BTC-e failed to conduct any due diligence on the

transactions or on the accounts in which the stolen bitcoin were held. Moreover, BTC-e failed to file any SARs on these transactions even after the thefts were publicly reported in the media.

C. Failure to File Suspicious Activity Reports

The BSA and its implementing regulations require an MSB to report transactions that the MSB "knows, suspects, or has reason to suspect" are suspicious, if the transactions are conducted or attempted by, at, or through the MSB, and the transactions involve or aggregate to at least $2,000 in funds or other assets.[15] A transaction is "suspicious" if the transaction: (a) involves funds derived from illegal activity; (b) is designed to evade reporting requirements; (c) has no business or apparent lawful purpose, and the MSB knows of no reasonable explanation for the transaction after examining the available facts, including background and possible purpose; or (d) involves use of the money services business to facilitate criminal activity.[16]

BTC-e processed thousands of suspicious transactions without ever filing a single SAR. Unreported transactions included those conducted by customers who were widely reported as associated with criminal or civil violations of U.S. law. For example, from November 14, 2013 through July 21, 2015, BTC-e processed over 1,000 transactions for the unregistered U.S.-based virtual currency exchange Coin.MX. Coin.MX's operator, Anthony R. Murgio, pled guilty to charges that included conspiracy to operate an unlicensed money transmitting business.[17] Coin.MX processed over $10 million in bitcoin transactions derived from illegal activity throughout its operations, including a substantial number that involved funds from ransomware extortion

[15] 31 U.S.C. § 5318(g)(1) and 31 C.F.R. § 1022.320(a)(2).

[16] 31 U.S.C. § 5318(g)(1) and 31 C.F.R. §§ 1022.320(a)(2)(i)-(iv).

[17] "Operator Of Unlawful Bitcoin Exchange Pleads Guilty In Multimillion-Dollar Money Laundering And Fraud Scheme," Department of Justice, U.S. Attorney's Office for the Southern District of New York, January 9, 2017, https://www.justice.gov/usao-sdny/pr/operator-unlawful-bitcoin-exchange-pleads-guilty-multimillion-dollar-money-laundering.

payments. Even after the conviction of Coin.MX's operator, BTC-e failed to conduct reviews of the transactions that BTC-e processed for Coin.MX and failed to file any SARs.

Criminals, and cybercriminals in particular, used BTC-e to process the proceeds of their illicit activity. This was particularly the case for some of the largest ransomware purveyors, which used BTC-e as a means of storing, distributing, and laundering their criminal proceeds. FinCEN has identified at least $800,000 worth of transactions facilitated by BTC-e tied to the ransomware known as "Cryptolocker," which affected computers in 2013 and 2014. Further, over 40 percent of all bitcoin transactions, over 6,500 bitcoin, associated with the ransomware scheme known as "Locky" were sent through BTC-e. Despite readily available, public information identifying the bitcoin addresses associated with Locky, BTC-e failed to conduct any due diligence on the recipients of the funds and failed to file SARs.

BTC-e also failed to file SARs on transactions that involved the money laundering website Liberty Reserve. Liberty Reserve was a Costa Rica-based administrator of virtual currency that laundered approximately $6 billion in criminal proceeds. Liberty Reserve's website was seized by the U.S. government and shut down when its owner and six other individuals were charged with conspiracy to commit money laundering and operating an unlicensed money transmitting business. FinCEN issued a finding under Section 311 of the USA PATRIOT Act that Liberty Reserve was a financial institution of primary money laundering concern.[18] Not only did BTC-e share customers with Liberty Reserve, "BTC-e code" was redeemable for Liberty Reserve virtual currency. BTC-e failed to file SARs even after the public shutdown of Liberty Reserve in May 2013.

[18] "Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311," Department of the Treasury, May 28, 2013, https://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx.

D. Recordkeeping Requirements

The BSA and its implementing regulations require MSBs and other non-bank financial institutions to obtain and retain records related to transmittals of funds in amounts of $3,000 or more.[19] BTC-e failed to collect even the most basic customer information and lacked adequate procedures for conducting due diligence and monitoring transactions. Transactional records maintained by BTC-e lacked critical information such as name, address, and account numbers.

IV. CIVIL MONEY PENALTY

FinCEN has determined that BTC-e willfully violated the BSA and its implementing regulations, as described in this ASSESSMENT, and that grounds exist to assess civil money penalties for these violations. FinCEN has determined that the proper penalties in this matter are a penalty of $110,003,314 imposed on BTC-e and a penalty of $12,000,000 imposed on Alexander Vinnik.

By:

/s/ 7/26/2017

Jamal El-Hindi Date:
Acting Director
FINANCIAL CRIMES ENFORCEMENT NETWORK
U.S. Department of the Treasury

[19] 12 U.S.C. § 1829b and 31 C.F.R. § 1010.410(e).

EXHIBIT C

STEPHANIE M. HINDS (CABN 154284)
United States Attorney
MICHELLE LO (NYRN 4325163)
Chief, Civil Division
SAVITH IYENGAR (CABN 268342)
Assistant United States Attorney

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
Telephone: (415) 436-7200
Fax: (415) 436-6748
savith.iyengar@usdoj.gov

Attorneys for the United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. BTC-e, a/k/a CANTON BUSINESS CORP., and ALEXANDER VINNIK, Defendants.	CASE NO. 4:19-cv-04281 KAW **STATUS REPORT**

Plaintiff United States of America (the "United States") respectfully submits this status report pursuant to the Court's Order dated April 22, 2022. *See* ECF No. 30.

As the United States previously reported to the Court, the United States completed service on defendants BTC-e, a/k/a Canton Business Corp., and Alexander Vinnik (collectively, "Defendants") under Federal Rule of Civil Procedure 4(f)(1) and the Hague Service Convention on November 18, 2021, and Defendants' response to the complaint was due within twenty-one (21) days thereafter, *i.e.*, on or before December 9, 2021, under Federal Rule of Civil Procedure 12(a)(1)(A)(i). *Id.* As of April 18, 2022, Defendants had failed to answer or otherwise respond to the complaint. *Id.* Accordingly, the United States respectfully requested that the Court allow the United States to file another status report in thirty (30) days, or by May 18, 2022, regarding whether Defendants have answered or otherwise

responded to the complaint, and stated that if Defendants had not responded to the complaint by that date, the United States would seek entry of default against any non-responding Defendant pursuant to Federal Rule of Civil Procedure 55. *Id.*

To date, Defendants have failed to answer or otherwise respond to the complaint. The United States intends to seek entry of default against Defendants pursuant to Federal Rule of Civil Procedure 55 no later than July 18, 2022. Should the Court require any further status updates in the meantime, the United States shall provide such updates as ordered by the Court.

Respectfully submitted,

STEPHANIE M. HINDS
United States Attorney

Dated: May 18, 2022

By: */s/ Savith Iyengar*
SAVITH IYENGAR
Assistant United States Attorney